Missouri Secretary of State Robin Carnahan
Records Services Division
presents:

Trustworthy Information Systems Approach

Workshop 4 in the Missouri Electronic Records Education and Training Initiative
June 7, 2005
Presented by:
John Breeden, CRM

Provided under contract with:
***e*Visory**

Outcomes

At the end of this session, you will understand:

- What is a trustworthy information system
- What makes an information system trustworthy
- Why it is important to have a trustworthy information system

2

Outcomes

In addition, you will understand:

- How to evaluate the trustworthiness of an information system using the ***Trustworthy Information Systems Handbook***
- How to use ISO 15801 criteria to ensure trustworthiness and reliability of an imaging system

3

What is a Trustworthy Information System?

Definition of Information System

- An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software (both operating system and application), information, data, communications, and people.

5

Trust and Trustworthy

Trust:

- To place confidence in; to rely on; to believe in the integrity; to place reliance on; to be confident

Trustworthy:

- Worthy of trust or confidence; dependable; reliable

6

Definition of Record

- Any document, book, paper, photograph, map, sound recording or other material, regardless of physical form or characteristics, made or received pursuant to law or in connection with the transaction of official business (RSMo 109.210.5).

7

Why Do We Keep Records?

Records Values

Informational/business value: Documents the unique functions and activities carried out by state and local government in the performance of their distinctive missions

Fiscal value: Documents financial obligations between government and citizens or other organizations

9

Records Values

Legal: Documents legally enforceable rights or obligations, both those of a government agency or other organization and those of persons directly affected by the agency's activities

Historical: Documents the activities of government that have continuing evidential or informational value

10

What Makes Trustworthy Information Systems

Trustworthy Information Systems

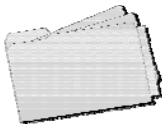
- Must have the following attributes:
  - Be authentic
  - Be reliable
  - Have integrity
  - Be accessible

12

Authenticity

An authentic record is one that is proven:

- To be what is purports to be
- To have been created or sent by the person purported to have created or sent it
- To have been created or sent at the time purported



13

Reliability

A reliable record is one:

- Whose contents can be trusted as a full and accurate representation of the transactions, activities, or facts to which they attest
- Can be depended upon in the course of subsequent transactions or activities

A record ceases to be reliable if, over time, some part of its content, structure or context has been lost

14

Integrity

A record that has integrity is one:

- That is complete and unaltered, or the changes (alterations, additions, or deletions) are a part of the business process and are documented and strictly controlled

15

Accessibility

A record that is accessible is one:

- That can be reliably retrieved in a timely fashion throughout the entire retention period

16

Why is it Important to Have Trustworthy Records?

- Enable us to provide better service to the public
- Provide confidence in government by the public
- Provide confidence that information can be retrieved for as long as it has value
- Protection from litigation
- Help us to perform our jobs more efficiently

17

Process for Establishing Trustworthy Information Systems

- Assemble team
- Determine importance of information in the system
- Choose criteria or components that apply to new or existing systems
- Implement
- Reassess

18

When to Undertake this Process

- Best time is in the initial system analysis and design
- When system is migrated to new versions
- Can be applied anytime

19

Assemble Team

- Business/end users - Determine the value of the information based on business needs
- Information technology - Provide advice on technologies and methodologies to accomplish business needs
- Other stakeholders including records management, audit, legal, security

20

Choosing Criteria for New Systems

- Determine the value of the information
- Weigh that value against the costs (time, money, etc.) of implementing each criteria
- Choose only those criteria that support your determined level of risk
- Implement
- Reassess needs and risks on a regular basis

21

Choosing Criteria for Existing Systems

- Examine your systems with reference to the criteria and determine which ones are already in place
- Weigh the value of modifying the system for additional criteria against the costs (time, money, etc.) of adding each new criteria
- Choose only those criteria worth the additional cost
- Implement
- Reassess needs and risks on a regular basis

22

Determining the Value of the Information

- What laws and regulations apply to your data?
- What are the requirements for system security, data security, and records retention?
- What areas and records might lawyers and auditors target?
- What data is of permanent and/or historical value to you and to others?

23

Who Do You Trust Quiz

Implementation

Criteria to Consider for Trustworthy Information Systems

- Documentation
- Security Measures
- Audit Trails
- Disaster Recovery Plans
- Metadata

26

Documentation

System documentation should include, but not be limited to:

- Hardware (procurement, installation, modifications, and maintenance)
- Software (procurement, installation, modifications, and maintenance)
- Communication networks (procurement, installation, modifications, and maintenance)
- Interconnected systems

27

Documentation Criteria

Criteria	*In Place? Yes / No*	*Planned? Yes / No*	*Rationale / Notes*
Performance and reliability testing of hardware and software on a schedule established through consultation with the manufacturers			

28

Documentation

Interconnected systems include:

- List of interconnected systems (including the internet)
- Names of systems and unique identifiers
- Owners
- Names and titles of authorizing personnel
- Dates of authorization
- Types of interconnection
- Indication of system of record
- Sensitivity levels
- Security mechanisms, security concerns, and personnel rules of behavior

29

Documentation

Policy and Procedure documentation should include, but not be limited to:

- Programming conventions and procedures
- Development and testing activities, including tools
- Applications and associated procedures, such as methods of entering/accessing data, data modification, data duplication, data deletion, indexing techniques, and outputs

30

Documentation

Policy and Procedure documentation should include:

- Identification of when records become official
- Record formats and codes
- Routine performance of system backups - each backup should be documented with backup media being appropriately labeled, stored in a secure, off-line, off-site location, and subjected to periodic integrity tests

31

Documentation

Policy and Procedure documentation should include:

- Routine performance of quality assurance and control checks, as well as performance and reliability testing of hardware and software on a schedule established through consultation with the manufacturers

32

Questions Break

Security Measures

User Identification/Authorization should include, but not be limited to:

- User identification and access procedures should be established and documented. Users should be authenticated prior to being granted access.
- Each user should be assigned a unique identifier and password. Identifiers and passwords should not be used more than once.

34

Security Criteria

Criteria	*In Place? Yes / No*	*Planned? Yes / No*	*Rationale / Notes*
Each user is assigned a unique identifier and password.			

35

Security Measures

User Identification/Authorization should include:

- Password rules should include standard practices such as minimum password length, expiration dates, and a limited number of log-on attempts. System administrators should determine what level and frequency of log-on error constitutes a misuse problem which, in turn, would trigger the notification of security personnel.

36

Security Measures

User Identification/Authorization should include:

- Users should be restricted to only the level of access necessary to perform their job duties
- Permission to alter disposition/retention codes, and/or to create, modify, and delete records should be granted only to authorized users with proper clearance. Modification of record identifiers is not allowed.

37

Security Measures

User Identification/Authorization should include:

- Access to private keys for digital signatures should be limited to authorized individuals
- Lists of all current and past authorized users and their privileges and responsibilities should be maintained. The current list should be reviewed on a regular schedule to ensure the timely removal of authorizations for former employees, and the adjustment of clearances for workers with new job duties.

38

Security Measures

User Identification/Authorization should include:

- Personnel duties and access restrictions should be arranged such that no individual with an interest in record content will be responsible for administering system security, quality controls, audits, or integrity-testing functions. No individual should have the ability to single-handedly compromise the system's security and operations.

39

Security Measures

Internal System Security should include, but not be limited to:

- Access to system documentation should be controlled and monitored
- Access to output and storage devices should be controlled and monitored
- Controls should be in place to ensure proper security levels of data when archiving, purging, or moving from system to system. Controls should be in place for the transportation or mailing of media or printed output.

40

Security Measures

Internal System Security should include:

- Procedures should be implemented to ensure the complete sanitization and secure disposal of hardware, software, and storage media when outdated or supplanted by newer versions, units, etc. Documentation should include date, equipment identifiers, methods, and personnel names.

41

Security Measures

Internal System Security should include:

- Security administration personnel should undergo training to ensure full understanding of the security system's operation
- Measures should be in place to guard the system's physical security. Items to consider include:
  - Access to rooms with terminals, servers, wiring, backup media
  - Data interception
  - Mobile/portable units such as laptops
  - Structural integrity of building
  - Fire safety
  - Supporting services such as electricity, heat, air conditioning, water, sewage, etc.

42

Security Measures

Internal System Security should include:

- Security-detection mechanisms should be constantly monitoring the system. Fail-safes and processes to minimize the failure of primary security measures should be in place at all times.

43

Security Measures

External System Security should include, but not be limited to:

- In cases of remote access to the system, especially through public telephone lines, additional security measures should be employed. Possible action could include the use of input device checks, caller identification checks (phone caller identification), call backs, and security cards.

44

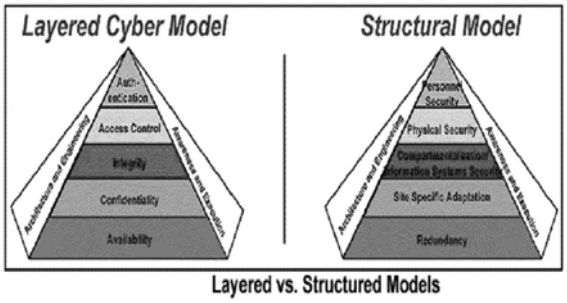
Security Measures

External System Security should include:

- For records originating outside the system, the system should be capable of verifying their origin and integrity. At a minimum, the system should:
  - Verify the identity of the sender or source
  - Verify the integrity of or detect errors in the transmission or informational content of the record
  - Detect changes in the record since the time of its creation or the application of a digital signature
  - Detect any viruses or worms present

45

FAA Security Model



Layered vs. Structured Models

46

Who Do You Trust Quiz

Audit Trails

General Characteristics of Audit Trails should include:

- Audit trail software and mechanisms should be subject to strict access controls and protected from unauthorized modification or circumvention
- Audit trails should be backed up onto removable media periodically to ensure minimal data loss in case of system failure
- System should automatically notify system administrators when audit storage media is nearing capacity and response should be documented. When the storage media containing the audit trail is physically removed from the system, the media should be physically secured as required by the highest sensitivity level of data it holds.

48

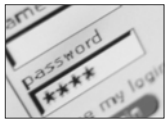
Audit Trail Criteria

Criteria	*In Place? Yes / No*	*Planned? Yes / No*	*Rationale / Notes*
Audit trails are backed up onto removable media periodically			

49

Audit Trails

- A system should be in place to track password usage and changes. Recorded events and information should include:
  - User identifier
  - Successful and unsuccessful log-ins
  - Use of password changing procedures
  - Date
  - Time
  - Physical location



50

Audit Trails

- A system should be in place to log and track users and their online actions. Audit information might include:
  - Details of log-in (date, time, physical location, etc.)
  - Creation of files/records
  - Accessed file/record identifiers and accompanying activity (deletion, modification, change of sensitivity/security level)
  - Accessed device identifiers

51

Audit Trails

- Log and track continued:
  - Software use
  - Production of printed output
  - Overriding of human-readable output markings (including overwrite of sensitivity label markings and turning off of labeling mechanisms) on printed output
  - Output to storage devices

52

Audit Trails

- For each record, audit trails should log, at a minimum, the following information:
  - Record identifier
  - User identifier
  - Date
  - Time
  - Usage (e.g., creation, capture, retrieval, modification, deletion)

53

Disaster Recovery Plans

- Elements of Disaster Recovery Plans:
  - Identifying vital records
  - Risk management processes
  - Hazards
    - Hardware, software, or network failure
    - Fire and/or explosion
    - Tornado, lighting, or hurricane
    - Violence and/or terrorism
    - Pests such as insects and rodents
    - Human error

54

Disaster Recovery Plans

- Elements of Disaster Recovery Plans:
  - Selecting protection methods and remote storage
  - Preparing a vital records schedule
  - Identifying corrective and preventive measures
  - Implementing measures for the protection of electronic records and information

55

Disaster Recovery Criteria

Criteria	*In Place? Yes / No*	*Planned? Yes / No*	*Rationale / Notes*
A vital records schedule has been prepared			

56

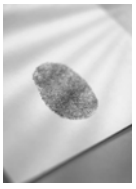
Metadata

- Type of metadata:
  - Identification
  - Access/Rights
  - Vital record status
  - Retention/disposition
  - History/Preservation/Migration Audit Trail

57

Metadata

- Identification:
  - Unique Identifier
  - Office or Organization of Origin
  - Author/Creator/Originator/Contributor(s)
  - Coverage/Scope
  - Date Created
  - Date Declared/Filed
  - Date Modified



58

Metadata

- Identification (cont):
  - Date Received/Acquired
  - Date Published/Available
  - Description/Abstract
  - Document Type
  - Format/Application
  - Location

59

Metadata Criteria

Criteria	*In Place? Yes / No*	*Planned? Yes / No*	*Rationale / Notes*
Date Received/ Acquired Retained			

60

Metadata

- Identification (cont):
  - From/Sender
  - Subject/Key Words
  - To/Addressee/CCC/BCC
  - Media Type
  - Record/Version/Rendition Number
  - Relationships/Links

61

Metadata

- Identification (cont):
  - Status (record or non-record)
  - User-Defined fields
- Vital Records:
  - Vital Record Indicator

62

Metadata

- Access/Rights Control:
  - Security Classification
    - Subject to Missouri Sunshine Laws
    - Exempt from Missouri Sunshine Laws
    - Critical Infrastructure Information
  - Other Access Condition
  - Usage
  - Encryption Details

63

Metadata

- Retention/Disposition:
  - Disposition action
  - Disposition action date
  - Disposition instruction
  - File Code/Number
  - Destruction hold

64

Metadata

- History/Preservation/Migration Audit Trail:
  - Change history (succession of values)
  - Date accessed
  - Date copied
  - Date moved
  - Date re-formatted
  - Storage media
  - Transaction log (who, what, when)

65

Who Do You Trust Quiz

Questions
Lunch

67

Trustworthy Document Imaging

68

Document Imaging Outline

- Policy documents
- Duty of care/security
- Procedures and processes
- Technology considerations
- Audit trails

69

Imaging Policies

- Policy document should contain:
  - What information is covered
  - Policy regarding storage media and version control
  - Policy regarding image file formats
  - Policy regarding relevant information management laws and standards
  - Procedures and processes

70

Imaging Policies

- What information is covered:
  - Information should be grouped into types or records series
  - The policy for all information within each type should be consistent

71

Imaging Policies

- Storage media and version control:
  - Different types of storage media have different long-term storage characteristics. The policy should identify the storage media, including if any information needs to be stored on more than one media.
  - Different versions must be tracked in order to ensure that no changes have been made

72

Imaging Policies

- Image file formats:
  - Contain details about the image file formats to be used for each information type
  - Where compression techniques are available, policy on their use should be documented

73

Imaging Policies

- Relevant laws and standards:
  - Retention schedules and disposition periods should be identified for each information type
  - All stakeholders should agree to the retention periods
  - All relevant system and procedural documentation should be included in schedule
  - Relevant laws and industry standards should be cited

74

Imaging Duty of Care

- It is essential that the government is aware of the value of information and executes its responsibility under the duty of care principle by:
  - Being aware of obligations to legislative or other legal bodies
  - Keeping up to date with technical, regulatory, and legislative changes by maintaining contact with those organizations

75

Imaging Duty of Care

- Value of information (cont):
  - Establishing a chain of accountability and responsibilities for activities:
    - Input reconciliation
    - Quality control
    - Data entry
    - Information deletion
    - Information security

76

Imaging Duty of Care

- Value of information (cont):
  - Identify which images are vital records
  - Identify vulnerabilities including rooms and computing devices that lack proper security
  - Implement disaster recovery plan including finding a "hot" site and offsite storage of duplicate software and images

77

Imaging Procedures and Processes

- The following procedures and processes should be included in a manual and implemented:
  - Document capture/scanning
  - Data capture
  - Indexing
  - Authenticated output procedures

78

Imaging Procedures and Processes

- (cont):
  - Document retention
  - Document destruction
  - Backup and system recovery
  - System maintenance
  - Security and protection

79

Document Image Capture

- May include the following sub-tasks:
  - Preparation of documents
  - Document batching
  - Photocopying
  - Scanning
  - Image processing

80

Document Image Capture

- Preparation of documents:
  - Examine to be sure a readable image can be obtained. Consider paper size, weight, binding, paper, print color, physical state, and contrast
  - Identify appropriate measure to capture the information including making copies of fragile documents and special image enhancement techniques
  - Incorporate in procedures manual

81

Document Image Capture

- Document batching:
  - Batch documents to facilitate scanning (by document type or by size)
  - Chose batch size to maximize quality control efficiency

82

Document Image Capture

- Photocopying:
  - Photocopy documents that would be damaged during the scanning process
  - Photocopy documents too large to be scanned into (overlapping) segments
  - If documents with embosses, signatures or other identifying characteristics were previously photocopied or photocopied as a part of the process, the document should be marked as such before scanning

83

Document Image Capture

- Scanning:
  - Procedures should ensure that all documents are scanned. Batching can facilitate the process if the system counts the images; discrepancies must be resolved.
  - Quality control and indexing processes may be used to ensure no documents were missed
  - It may be satisfactory to implement procedures where the probability and risk of a document not being scanned is acceptable

84

Document Image Capture

- Quality Control criteria should be determined based on value of the record and the risks if the quality is not sufficient
- May include the following:
  - Overall legibility
  - Smallest detail legibly captured (decimals, etc.)

85

Document Image Capture

- Quality Control criteria (cont):
  - Completeness of detail (broken characters, etc.)
  - Dimensional accuracy compared to the original
  - Scanner-generated speckle (when not on original)
  - Color fidelity

86

Document Image Capture

- Quality Control procedures:
  - A second person should evaluate quality even if the scanner operator is evaluating quality as they scan the documents. If a primary QC has been performed, the second QC can be performed by sampling rather than checking each image.
  - Records of quality control and rescanning should be maintained, including the batch, name of inspector, and date of inspection and rescan

87

Data Capture

- New Data:
  - New data may be captured in a number of ways, including manual (keyboard), automated (bar code, optical character recognition) or semi-automatically (auto and manual entry).
- Migration:
  - Receiving data from other systems is often more efficient. Procedures and processes should be documented when data files and associated metadata are received from another system.

88

Who Do You Trust Quiz

Questions Break

Indexing

- Indexing is a vital part of the process of storing information on electronic media. It allows access to the information. When indexing information is lost, the stored information can be lost.
- The following should be considered:
  - Manual or automatic indexing
  - Index storage
  - Index accuracy

91

Indexing

- Manual or automatic indexing
  - Manual indexing can be performed pre- and post-scanning. Staff should receive training and constant quality control monitoring is required. Auto indexing is less likely to result in error but QC should still be performed.
- Index storage
  - Retain index data as long as the image is retained. Delete indices of expunged information.

92

Indexing

- Index accuracy
  - Criteria for index accuracy should be realistic considering method used. Accuracy expectations should be documented and measured.
  - Consider the risks (can't find information, litigation) and costs when establishing indexing accuracy levels

93

Authenticated Output Procedures

- Output, either in the form of paper or electronic files, may need to be reproduced for use as documentary evidence. Generally these copies need to be authenticated as true copies to reduce the likelihood of rejection or challenge. The audit trail metadata can be key to gaining acceptance.

94

Document Retention

- Typically originals are destroyed after they have been scanned, in accordance with an approved retention schedule. Destruction should be suspended when fraud has been identified or litigation eminent or ongoing.
- Originals should also be retained for the following reasons:
  - Original has historic significance
  - Source documents contain annotations or other information characteristics that could not be captured or documented but retain legal or other value

95

Document Destruction

- Procedures for the destruction of documents at the end of the retention period should be documented. They should incorporate the following:
  - Destruction should take into account sensitivity of the information being destroyed
  - No source documents should be destroyed until QC has been performed, the images have been written to the media, and a backup has occurred

96

Backup and System Recovery

- System should allow backup at regular intervals
- Backup data must include associated information such as index files and audit trails
- Procedures should include secure, off-site storage of backup media
- Media used for backups do NOT provide guarantees for the preservation of permanently valuable records. Consider using more permanent media such as microfilm.

97

System Maintenance

- The image system should be maintained only by qualified personnel to ensure that the integrity of the images captured or created and stored is not affected by the equipment
- System hardware, software, and media should be migrated to current versions while retaining existing metadata and metadata of migration

98

Security and Protection

- Security Procedures
  - A secure access control system should be implemented to ensure proper access to the various levels of the systems (e.g. manager, data input, data deletion, and retrieval)
  - The system should be set up in secure locations (servers in tightly controlled areas) and all hardware and indexing workstations set up with password protection

99

Security and Protection

- Encryption keys and digital signatures
  - Encryption techniques may be used to improve security and integrity of stored data
  - Digital signatures consist of data which, when appended to the file, enables the user of the file to authenticate its origin and integrity

This probably won't be necessary for most systems if other safeguards are in place

100

Who Do You Trust Quiz

Technology Considerations

- Has the following subcategories:
  - Storage media and sub-system considerations
  - Access levels
  - System integrity checks
  - Image processing
  - Compression techniques

102

Technology Considerations

- Subcategories (cont):
  - Forms overlay and removal
  - Environmental considerations
  - Migration
  - Expungement

103

Technology Considerations

- Storage media and sub-system considerations:
  - The risk of storage media and information being tampered with. It is more difficult to commit fraud with write once media than with magnetic media.
  - Regardless of media used, procedures should be implemented to minimize the chance of unauthorized modifications

104

Technology Considerations

- Access level sub-system considerations:
  - System access rights should be granted only after the staff member has successfully proved their competence. Only staff with relevant access rights should be permitted to enter or amend stored data.
  - Examples of levels of access:
    - system manager, system administrator, authors/originators/scanner operators, indexers, varying levels of retrieval access

105

Technology Considerations

- System integrity checks:
  - Protect hardware from power failure (UPS)
  - Virus and worm protection software should be kept up to date
  - Facilities, such as the use of checksum, should be provided to ensure the integrity of the information
  - Digital and other electronic signatures can be stored with the files to which they are bound

106

Technology Considerations

- Image processing techniques can be used to improve recognition rates for automated data capture or improve the appearance of an image. However, it is important that there be no loss of information or the integrity of the image be compromised.
- Image processing techniques include:
  - De-skew, de-speckle/background cleanup, and forms removal

107

Technology Considerations

- Compression techniques
  - Compression techniques can affect the integrity of the images, but can reduce storage space and speed retrieval.
  - Compression can either be "lossless" or "lossy". Lossy compression should be used with care because information is removed during the compression process, leading to possible questions about authenticity.

108

Technology Considerations

- Compression techniques (cont)
  - Lossy compression may be suitable for continuous tone material such as photos where there is no significant loss of information. Perform careful quality control to ensure information loss is acceptable.
  - Lossy compression is not recommended for medical and engineering X-ray images
  - Consider storing images both ways-one for rapid retrieval and the other for authenticity

109

Technology Considerations

- Forms overlay and removal

  Some imaging applications automatically remove the form from the image to save storage space and improve transmission speeds. Prior to implementing these systems:
  - Determine whether the form needs to be retained to be overlaid over the information
  - Document the process to improve acceptance of these images in court

110

Technology Considerations

- Environmental considerations
  - Manufacturer's environmental (heat, humidity, air quality) recommendations should be be followed for all hardware, software, and media
  - Media handling and storage procedures should be followed
  - All media have a finite life, making regular checking of the media in accordance with manufacturer's recommendations necessary

111

Technology Considerations

- Migration

  Many images must be retained for longer than the life of the hardware, software and media. To ensure the integrity of the stored information, plan for as many migrations as will be necessary (one every 3-6 years) to meet the required retention.

112

Technology Considerations

- Migration
  - Use standard image formats and maintain/upgrade hardware/software to retrieve the information
  - Plan to migrate metadata, index data, and audit trails to new technology without loss of integrity and with sufficient migration documentation to allow the integrity of the stored information to be established at any time in the future

113

Technology Considerations

- Expungement
  - The system should have ability to expunge (delete) an image as well as amend (annotate and mask portions) the image
  - Adequate safeguards, procedures, and audit trails should be in place when amendments or expungements are performed
  - It may not be acceptable to only remove the image index on WORM media

114

Audit Trails

- The following features of audit trails are important:
  - Creation
  - Date and time
  - Access
  - Security and protection
  - Migration/Conversion
  - File Information
  - Indexing
  - Destruction
  - Workflow

115

Audit Trails

- Creation:
  - Audit trail data should be generated automatically from the system as much as possible
  - Consider whether audit trails should be maintained on drafts temporarily or permanently

116

Audit Trails

- Date and time:
  - Each audit trail data should have a date and time identifying when it was stored
  - The date and time will normally be the creation of the metadata but should closely match the event being documented

117

Audit Trails

- Access:
  - Audit trail information must be accessible to system administrators, but need not be made accessible to all users
  - Audit trail information must be available for inspection by external personnel (such as auditors) who may have little familiarity with the system

118

Audit Trails

- Security and protection:
  - The audit trail may be fundamental in establishing the authenticity of questioned information
  - Audit trail information kept within the system should not be modifiable
  - Secure backup copies of the audit trail should be kept
  - For least risk, store metadata on WORM media

119

Audit Trails

- Migration/Conversion:
  - Where information has been converted from one file format to another, details of the conversion should be stored in the audit trail
  - In the case of Hierarchical Storage Management (HSM) systems, where data is routinely moved between storage devices without user intervention, it may not be necessary to generate audit trails of this movement

120

Audit Trails

- File Information:
  - Unique file identifier
  - Number of documents/pages in the file
  - Size of the file (50.5 kilobytes, etc.)
  - File format
  - File code (DTD, etc.)

121

Audit Trails

- Indexing:
  - Date and time of the creation, amendment, and modification of index should be generated
  - Where an index item relates to deleted or expunged information, this fact should be documented

122

Audit Trails

- Destruction:
  - Audit trail data should be kept for the destruction of source documents following document scanning
  - Audit trail data should be kept for the destruction of information at the end of the relevant retention period
  - Audit trail data should be kept of the authorization of destruction

123

Audit Trails

- Workflow:
  - In most workflow systems, an audit trail point exists at each step in the workflow. The user should decide which audit trail points are relevant and for how long
  - The selected audit trail points may change as the workflow processes change
  - The system should permit an authorized user to select and deselect audit trail points for which audit trail data are generated

124

Who Do You Trust Quiz

Some Points to Remember

- Trustworthy information systems have integrity and are authentic, reliable, and accessible
- The building blocks of trustworthy systems are
  - documentation
  - proper security measures
  - good audit trails
  - good metadata
- You can apply these building blocks to develop trustworthy imaging systems

126

For Help

Missouri Secretary of State Records Services Division:
http://www.sos.mo.gov/records/

Records Management 573-751-3319

Local Records 573-751-9047

127

For More Help

Minnesota Trustworthy Information System:
http://www.mnhs.org/preserve/records/

International Standards Organization (ISO) 15801, recommendations for trustworthiness and reliability:
http://www.iso.org

128

Questions?

John Breeden, CRM
JLJBreeden@aol.com
804-338-6384